UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

| | | |
|---|---|---|
| UNITED STATES | * | |
| | * | |
| v. | * | Criminal Action No. 1:20-cr-10012-IT |
| | * | |
| PAUL BATEMAN, | * | |
| | * | |
| Defendant. | * | |

MEMORANDUM & ORDER

July 20, 2021

TALWANI, D.J.

Pending before the court is Defendant Paul Bateman's Motion to Compel Discovery [#76]. For the following reasons, the motion is DENIED.

## I. Background

On December 11, 2019, Homeland Security Investigations ("HSI") Special Agent Squire presented an affidavit in support of an application for a search warrant of Bateman's home. Squire Aff. 30 [#76-4]. According to the affidavit, Website A was a child pornography site that operated on Tor[1] as a hidden service—a website accessible only to users operating within the Tor network—from at least September 2016 through June 2019. Id. at ¶¶ 11, 14-15. Like other websites, hidden services are globally accessible, and their users may be located anywhere in the world. Id. at ¶ 22.

The affidavit explains that during an investigation into Website A, a foreign law enforcement agency ("FLA") determined that on April 20, 2019, the IP address 73.142.30.140

[1] "Tor" refers to the onion router, a network that facilitates efforts to anonymize communications over the Internet by routing Tor user communications through a globally distributed network of intermediary computers. Id. at ¶ 6.

was used to access child pornography hosted on Website A. Id. at ¶ 23. The affidavit states that this information was obtained by the FLA "through independent investigation that was lawfully authorized in the FLA's country pursuant to its national laws." Id. at ¶ 25. The affidavit further states that the FLA "had not interfered with, accessed, searched, or seized any data from any computer in the United States in order to obtain that IP address" and that "U.S. law enforcement personnel did not participate in the investigative work" through which the FLA identified the IP address. Id. According to publicly available information, IP address 73.142.30.140 is owned and operated by Comcast Communications ("Comcast").[2] Id. at ¶ 27.

According to the affidavit, when a law enforcement agency obtains evidence that a user of a hidden service like Website A is located in another country, it is common practice for that law enforcement agency to share information with the law enforcement agency in the country where the user appears to be located. Id. at ¶ 22. The FLA followed this practice and shared the information about this IP address with U.S. law enforcement. Id. at ¶ 25.

On September 10, 2019, an administrative subpoena was issued to Comcast for information regarding which of its customers had IP address 73.142.30.140 on April 20, 2019. Id. at ¶ 27. Comcast provided Bateman's name and address. Id.

Based on Squire's affidavit, HSI obtained a search warrant for Bateman's home, which was executed on December 12, 2019. Squire Aff. in Support of Complaint ¶ 4 [#1-1]. According to law enforcement, Bateman was present, waived his Miranda rights, and made several incriminating statements. Id. at ¶¶ 5-6. During the search, Bateman directed law enforcement agents to an encrypted hard drive with an encrypted container, in which Bateman stored child

[2] IP addresses are not owned by individual users. Rather, the vast majority are owned by Internet service providers, who then effectively lease the IP addresses to their customers.

pornography. Id. at ¶ 7. Bateman told the agents how to decrypt the hard drive and the container, in which agents located a considerable amount of child pornography. Id. at ¶¶ 7-9.

Bateman was arrested and subsequently indicted on one count of receipt of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), and one count of possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2). Indictment [#11].

The government provided Bateman with automatic discovery, including, among other things, the search warrant and Squire's supporting affidavit. See Status Report [#21]. The case was scheduled for a Rule 11 hearing, but the hearing was cancelled at Bateman's request. Assented-to Mot. to Cancel Rule 11 Hearing [#52]. Bateman then requested additional discovery from the government by letter dated February 2, 2021, to which the government responded on February 16, 2021, agreeing to provide some of the requested discovery. See Mot. to Compel 3 [#76]. Bateman sent a second discovery letter on April 12, 2021, to which the government responded on April 26, 2021. Id.; Apr. 26, 2021 Letter [#76-1]. Bateman filed the pending Motion to Compel Discovery [#76] on May 25, 2021.

## II. Legal Standard

Federal Rule of Criminal Procedure 16(a)(1)(E) requires the government to permit, upon the defendant's request, inspection of items within the government's control if: (1) the item is material to preparing the defendant's defense; (2) the government intends to use it in its case-in-chief; or (3) the item belongs to the defendant. Fed. R. Crim. P. 16(a)(1)(E). "[A] showing of materiality requires 'some indication' that pretrial disclosure of the information sought 'would [] enable[] the defendant significantly to alter the quantum of proof in his favor.'" United States v. Goris, 876 F.3d 40, 45 (1st Cir. 2017) (quoting United States v. Ross, 511 F.2d 757, 763 (5th

Cir. 1975)). "This significant alteration may take place in a myriad of ways, such as 'uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal.'" Id. (quoting United States v. Lloyd, 992 F.2d 348, 351 (D.C. Cir. 1993)).

## III. Discussion

Bateman seeks disclosure of the following:

(1) identification of the members of the "multinational, multi-agency working group that coordinates national and international operations to combat child exploitation on the dark web" referenced in Squire's affidavit in support of the search warrant;

(2) information regarding the investigative technique used by the FLA to identify the IP address that accessed Website A on April 20, 2019;

(3) information regarding the location of the Consulate General from which the FLA's tip appears to have been sent; and

(4) documentation of communication between the FBI and HSI regarding the FLA tip.

Apr. 26, 2021 Letter [#76-1]. Bateman argues that this discovery would enable him to determine (1) whether Squire provided misleading information regarding the collaboration between the United States and the FLA in his affidavit in support of the search warrant, and (2) whether the means used to discover his IP address violated his Fourth Amendment rights. Mot. to Compel 2 [#76].

First, Bateman claims that he has a "good faith basis to suspect that the affidavit contains materially false or misleading information about the nature of the FLA investigation." Mot. to Compel 2 [#76]. Pointing to several public sources, including blog posts and the FLA's website and social media, Bateman argues that there is an ongoing collaboration between the FLA and the United States to combat the sexual exploitation of children. Id. at 21. He also cites Squire's own affidavit in support of the search warrant, which states that Squire is "an active member of a

multinational, multi-agency working group that coordinates national and international operations to combat child exploitation on the dark web." Id. at 23. In addition, Bateman points out that the letter from the FLA to the FBI, which states that the FLA provided the FBI with IP addresses during an "independent investigation" that was "lawfully authorized" by its own government, is dated September 16, 2019, six days *after* HSI issued an administrative warrant to Comcast to obtain Bateman's identity. Id. at 6. He argues that the letter was drafted post-hoc to support the government's litigation position. Id. Given this, Bateman asserts that the FBI was likely working with the FLA on the investigation of Website A and that Squire's affidavit therefore misrepresents the nature of the relationship between the law enforcement agencies. Id. at 23. The government counters that this is all speculation and that the fact that "the FLA and the United States have a collaborative relationship at various levels" in investigating child pornography does not mean that they collaborated in obtaining the user's IP address in this particular case. U.S. Opp. 4 [#81].

Next, Bateman argues that the requested discovery is critical to his ability to "challenge the search warrant that the government obtained in this case." Mot. to Compel 20 [#76]. Specifically, he claims that the likely collaboration between the United States and the FLA suggests that the means used to obtain his IP address may be subject to the Fourth Amendment's prohibition of unreasonable searches. Id. The government counters that the lawful means of obtaining this information is not material and that Bateman's requests are based on a theory of unlawful conduct too speculative to warrant approval. U.S. Opp. 4 [#81].

Beginning with the joint venture theory, "[o]rdinarily, the Fourth Amendment's exclusionary rule does not apply to foreign searches and seizures, for 'the actions of an American court are unlikely to influence the conduct of foreign police.'" United States v. Valdivia, 680

F.3d 33, 51 (1st Cir. 2012) (quoting United States v. Hensel, 699 F.2d 18, 25 (1st Cir. 1983)). "There are, however, two well-established exceptions to this rule: (1) where the conduct of foreign police shocks the judicial conscience, or (2) where American agents participated in the foreign search, or the foreign officers acted as agents for their American counterparts." Id. (quoting United States v. Mitro, 880 F.2d 1480, 1482 (1st Cir. 1989)).

Bateman argues that if such a joint venture existed, the fruits of the search—the evidence on his hard drive—would need to be suppressed if the search was not "reasonable" with the meaning of the Fourth Amendment. Mot. to Compel 23 [#76]. Bateman explains that there are several known instances in which United States law enforcement investigating child pornography websites on Tor has been able to identify users through "network investigative techniques" ("NITs") which, as a practical matter, amount to government installation of malware[3] on a user's computer. See, e.g., United States v. Tagg, 886 F.3d 579, 583 n.2 (6th Cir. 2018) (referring to the FBI's technique of installing a "benevolent virus" on a user's computer to obtain the computer's IP address). Because individuals have a reasonable expectation of privacy in the contents of their personal computers, use of such techniques requires a search warrant. See id. at 584 ("plac[ing] a digital bug [that infects the user's computer] in the fabric of the website . . . counts as a Fourth Amendment 'search' of the user's home computer"); see also United States v. Anzalone, 208 F. Supp. 3d 358, 366 (D. Mass. 2016), aff'd, 923 F.3d 1 (1st Cir. 2019) ("Even if the defendant did not have a reasonable expectation of privacy in [his IP address], he did have a reasonable expectation of privacy in the computer that housed this data and that was instructed by the NIT to transmit the data back to the government").

[3] Malware is the collective name for different types of software, such as worms, viruses, bots, and spyware, that are used to gain unauthorized access to or to damage a computer.

Bateman claims that the discovery he seeks might allow him to show that his IP address was discovered through the installation of malware on his computer in violation of the Fourth Amendment. Mot. to Compel. 2 [#76]. The government again counters that Bateman's argument is purely hypothetical and that he has "proffered no persuasive reason to doubt the FLA's statement that it did not interfere with a computer in the United States to identify the defendant's IP address as having accessed Website A." U.S. Opp. [#81].

The court agrees with the government. In effect, Bateman's argument is a stack of hypotheticals:

(1) the FLA may have misrepresented its lack of interference with a computer in the United States;

(2) Squire may have misrepresented the working relationship between the United States and the FLA; and

(3) a NIT may have been used in a joint venture to obtain Bateman's IP address.

All of Bateman's requests are based entirely on speculation that the evidence may show wrongdoing by foreign and domestic law enforcement. Such speculation does not satisfy the required showing of materiality that the discovery sought would "significantly to alter the quantum of proof" in Bateman's favor.

## IV. Conclusion

For the forgoing reasons, Bateman's Motion to Compel Discovery [#76] in DENIED.

IT IS SO ORDERED.

July 20, 2021

/s/ Indira Talwani
United States District Judge